Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

Del 11: Sikkerhetskultur og sikkerhetsledelse

Oppgave 1: Bygging av sikkerhetskultur

a. Ta utgangspunkt i dimensjonene for sikkerhetskultur beskrevet i avsnitt 13.1 i læreboka. Nevn eksempler på dårlig sikkerhetskultur for de forskjellige dimensjonene.
b. Med utgangspunkt i eksemplene fra a: Foreslå tiltak for å forbedre sikkerhetskulturen.
c. Foreslå mulige strategier som er egnet til å styrke kunnskap, motivasjon, holdninger og atferd med hensyn til informasjonssikkerhet for følgende kategorier av ansatte i en organisasjon:
   i) motiverte
   ii) likegyldige
   iii) misfornøyde
   iv) hemmelige agenter for fremmede stater

   Hvordan kan ulike strategier anvendes når det er uvisst hvilken kategori hver ansatt passer inn i, eller bør man forsøke å utforme en strategi som passer for alle kategorier av ansatte?

Løsningsforslag

a. Det fins uendelig mange eksempler, her er noen:
   1. Du forstår ikke hva phishing-epost er.
   2. Du jobber på et sykehus snakker med familie og venner om pasienter der.
   3. Du finner en minnepinne vet at man ikke skal plugge de inn, men er nysgjerrig og gjør det likevel.
   4. Du vet ikke om det fins en policy for minnepinner, så du plugger inn når du finner en, for du har ikke hørt at man ikke skal gjøre det.
   5. Du vet at skjermen skal låses når du forlater kontoret, men lar være fordi «du skal jo bare ut en kort tur»
   6. Du ser at en kollega har forlatt kontoret med innlogget skjerm som bryter policyen, men nevner det likevel ikke for ham for ikke å lage dårlig stemning.
   7. Du skjønner for sent at du har klikket på en lenke i en phishing epost, men later som intet har skjedd og forteller det ikke til noen.
   8. Du har en fil på din PC med alle dine passord i klartekst.
   9. Du lar partner/barn bruke din jobb-PC til all slags nettsurfing.
   10. Du syns sikkerhet er noe herk, og vil bare få jobben gjort.
   11. Du planlegger å bytte jobbe, og kopierer og tar med kundelister og bedriftssensitiv informasjon før du slutter.

b. Sikkerhetskultur er en del av virksomhetskulturen. Det er vanskelig eller umulig å oppnå en god sikkerhetskultur hvis det hersker en dårlig virksomhetskultur generelt, med en betydelig andel likegyldige eller misfornøyde ansatte. Virksomheten må derfor sørge for å ha en positiv virksomhetskultur fordi det er en forutsetning for å kunne bygge en sterk sikkerhetskultur. Hvis man antar at

virksomhetskulturen er tilstrekkelig god, er tiltak for forbedring av sikkerhetskulturen stort sett opplæring/bevissthetstrening, der spesifikke tiltak er nevnt i avsnitt 13.2 i læreboka, og som er hentet fra NSM sin veileder: https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/

- Gjennomfør balanserte sikkerhetstiltak og rutiner som tilsvarer behovet virksomheten har for sikkerhet, f.eks. basert på trussel- og risikovurdering.
- Virksomhetens leder og ledelse må involveres og gå foran som gode eksempler på god sikkerhetsatferd.
- Skap forståelse i hele organisasjonen hvorfor sikkerhet er viktig.
- For å kunne endre noe, må vi vite hva standpunkt er. Finn målbare forbedringspunkter i virksomheten for å se om forbedringstiltakene fungerer.
- Sett søkelys på enkelte områder som kan forbedres og bruk ulike virkemidler for å motivere de ansatte til å forbedre seg.
- Mål endringer underveis.
- Ros fungerer bedre enn ris.
- Evaluere, kommunisere og gjenta.

c. Tiltak for sikkerhetskultur kan ha ulik effekt for de ulike kategoriene ansatte.
   i) Ansvarsfulle er i stor grad mottakelig for og vil respondere godt på alle tiltakene nevnt i punkt b,
   ii) Likegyldige ansatte vil respondere dårlig på tiltakene nevnt i punkt b. Det kan være nyttig å identifisere denne typen ansatte, og gi dem særskilt oppfølging.
   iii) En misfornøyd ansatt kan ha tendens til å bevisst ignorere tiltak, eller kanskje (passivt) motarbeide tiltak, uten at den ansatte dermed er direkte innsidetrussel. Det kan være nyttig å identifisere denne typen ansatte, og gi dem særskilt oppfølging.
   iv) En agent for en fremmed stad har sin egen skulte agenda, som ikke tar hensyn til virksomhetens policyer. Det er ønskelig, men samtidig utfordrende å identifisere denne typen ansatte. Ved mistanke kan det være nyttig å samarbeid med PST. Oppfølging bør skje raskt og effektivt.

Oppgave 2: Innsidetrusselen

a. I perioden fra å bli ansatt til å slutte i et selskap, når er det størst sannsynlighet for at en ansatt blir en innsidetrussel?
b. Tiltak for å bygge holdninger og personlig integritet kan bidra til å forhindre at anstte blir en innsidetrussel. Hva er en type innsidetrussel som er lite påvirkelig for denne typen tiltak?

Løsningsforslag

a. Det er størst sannsynlighet for at en ansatt blir en innsidetrussel i forbindelse med at den ansatte forlater virksomheten, særlig ved oppsigelse eller avskjedigelse, men også når den ansatte frivillig slutter.
b. En ansatt som er hemmelig agent for en fremmed stat er lite påvirkelig for tiltak til styrking av sikkerhetskultur og holdninger.

Oppgave 3: Sosial manipulering

a. Beskriv måter å bruke sosial manipulering på for
   - å installere skadevare på PC-en til administrerende direktør i et selskap
   - å få uautorisert tilgang til bygningen for selskapets hovedkontor

b. Tenk deg at ansatte utgjør menneskelig «IDS» (Intrusion Detection System) mot sosiale manipuleringsangrep. Hva ville være en «falsk positiv» og en «falsk negativ» deteksjon av sosial manipulering? Vurder potensiell alvorlighet av falsk positiv og falsk negativ deteksjon av sosial manipulering.

c. Hva bør du gjøre hvis du tror du er blitt lurt av sosial manipulering?

Løsningsforslag

a. Eksempler på angrep gjennom sosial manipulering er:
   1. Tilgang til en bygning kan f. eks skje gjennom
      - «tailgating» bak andre, f.eks. etter lunsjpausen, eller følge etter de som har vært ute for å røyke sigaretter,
      - komme bærende med tunge bokser og få hjelp til å åpne døren
      - vise fram et falskt adgangskort
   2. Installere skadevare på computeren til konsernsjefen kan f.eks. skje gjennom:
      - å sende tilpassede spyd-phising e-post med vedlagt skadevare med mål om sjefen installerer og kjører skadevaren,
      - Sende tilpassede spyd-phishing e-post med vedlegg eller lenke til nettsted som inneholder en exploit som benytter en «Zero-Day» sårbarhet som fins på konsernsjefens computer.

b. En «falsk positiv» er når en legitim autorisert person stoppes. En «fallsk negativ» er når en angriper ikke blir stoppet.

c. Her er noen tiltak hvis du er blitt lurt eller er offer for identitetstyveri:
   - Hvis du har utført handlinger forespurt av en phisning epost eller en svindelnettside bør du kontakte helpdesk eller en annen relevant enhet.
   - Hvis du har oppgitt sensitive, personlig eller økonomisk informasjon bør du umiddelbart endre passord for berørte kontoer. Hvis du bruker samme passord for flere kontoer og nettsteder, kan du endre det for hver konto. Ikke bruk samme passord i fremtiden. Se etter tegn på identitetstyveri ved å gå gjennom bank og kredittkortutskrifter for mulige uautoriserte kostnader og aktiviteter. Hvis du merker noe uvanlig, må du umiddelbart kontakte banken. Vurder å rapportere angrepet til politiet.
   - Hvis du har mistet tilgang til en konto fordi en angriper har endret passord og andre detaljer slik at du er blitt utestengt må du få kontoen sperret ved å kontakte tjenestetilbyder per epost eller telefon.

Oppgave 4: Case om sikkerhetskultur

Din bedrift er i en sektor som typisk er utsatt for digitale sikkerhetstrusler. Policyer for informasjonssikkerhet fins, men ledelsen har ikke informert ansatte om disse. På pub etter jobben enn dag snakker du og noen kollegaer om informasjonssikkerhet i bedriften. En kollega nevner at når han mottar en phishing-epost, klikker han ofte på lenker og åpner vedlegg for moro skyld. Du syns det er dumt å gjøre, men sier intet fordi du ikke ville kritisere ham. Din kollegas holdning til phishing-eposter gjør deg urolig, så dagen etter snakker du med IT-drift om at en kollega klikker på phishing lenker for moro skyld. Du får til svar at så lenge det ikke har skjedd noe, trenger man ikke være urolig, og du at gjerne kan ta kontakt hvis du tror du er blitt lurt og det faktisk har skjedd noe.

a. Nevn aspekter du mener reflekterer dårlig sikkerhetskultur.
b. Gi forslag til hvordan sikkerhetskulturen kan forbedres, ikke bare ved å endre på de negative aspektene i a), men hvilke generelle tilnærminger for sikkerhetskultur som kan benyttes.

Løsningsforslag

a) Aspekter som viser dårlig sikkerhetskultur:

- Ledelsen sørger ikke for ansatte er oppmerksomme på sikkerhetspolicyene.
- Det er uakseptabelt å snakke om firmaets informasjonssikkerhet på pub blant andre folk.
- Kollegaen forstår ikke risikoen ved å klikke på lenker og åpne vedlegg i phishing eposter.
- Du forstår ikke at det er viktig å påpeke svakheter i sikkerhetskulturen hos kollegaer.
- IT-drift tar ikke hendelsen alvorlig, og forstår ikke at det faktisk er et sikkerhetsavvik å klikke på lenker og åpne vedlegg i phishing eposter.
- IT-drift forverrer sikkerhetskulturen når de forteller at det ikke er alvorlig å klikke ukritisk på lenker.
- Firmaet har tydeligvis ikke et system for avviksrapportering

b) Forslag til forbedring av sikkerhetskulturen:

- Ledelsen må kommunisere viktigheten av sikkerhetskultur
- Ansatte må få opplæring i sikkerhetskultur.
- Ansatte må si fra til hverandre når de gjør sikkerhetsfeil.
- Kjør simulerte phishing-angrep.
- Heng opp plakater.
- Sørg for at ansatte ikke er redd for å rapportere hendelser

Oppgave 5: ISMS

a. Hvordan er standardene ISO/IEC 27001 og ISO/IEC 27002-relatert?
b. Hva betyr "system" i forkortelsen ISMS (Information Security Management System) (Ledelsessystem for informasjonssikkerhet)?
c. Hvilken av ovennevnte standarder danner grunnlag for sertifisering, og hvorfor?
d. Hvordan bør en organisasjon avgjøre hvilke sikkerhetstiltak som skal implementeres?

Løsningsforslag

a. ISO/IEC 27001 beskriver krav til et ISMS (Styringssystem for informasjonssikkerhet), det vil si et rammeverk for å etablere og forvalte et sikkerhetsprogram i organisasjoner. ISO/IEC 27002 er en tiltaksbank for informasjonssikkerhet som organisasjoner kan vurdere å implementere som del av et ISMS.
b. ISMS beskriver hvordan organisasjoner kan styre info-sikkerhet på en systematisk måte, som er grunnen til å si at ISMS er et «system». ISMS oversettes både som ledelsessystem for informasjonssikkerhet, og styringssystem for informasjonssikkerhet.
c. Organisasjoner kan bli sertifisert etter ISO/IEC 27001, ikke etter ISO/IEC 27002. Årsaken er at ISO/IEC 27001 beskriver spesifikke krav til styring av informasjonssikkerhet, noe som vil være mer eller mindre likt for alle organisasjoner, og som kan revideres av en ekstern part. ISO/IEC 27002 beskriver et stort antall forskjellige sikkerhetstiltak, hvor ikke alle tiltak alltid er relevante for en organisasjon, fordi det avhenger av trussel- og risikobildet for hver organisasjon. Men det er selvsagt mulig å sjekke at trussel- og risikovurderinger er gjort, og at relevante sikkerhetstiltak er på plass, som vanligvis utføres av IT-sikkerhetsrevisorer.
d. Det fins hovedsakelig tre kilder til å identifisere sikkerhetstiltak som bør implementeres:
    1) Vanlig god praksis, dvs. sikkerhetstiltak som alltid trengs. Eksempler er brukerautentisering og tilgangskontroll. Men å beslutte garantinivåer for brukerautentisering, og spesifikke løsninger for tilgangskontroll kan bestemmes utifra risikovurderinger.
    2) Risikovurdering brukes til å bestemme områder der det er nødvendig å innføre sikkerhetstiltak. De mest kost-effektive tiltak velges for å mitigere risikoen.
    3) Lover og forskrifter som gjelder for en virksomhet kan diktere sikkerhetstiltak som er nødvendig å innføre for å ha etterlevelse.

Oppgave 6: Kategorisering av informasjonssikkerhetstiltak

Standarder og veiledere som beskriver informasjonssikkerhetstiltak benytter ulike kategoriseringer av sikkerhetstiltakene. Tre vanlige kategoriseringer er:

- Prosesskategorier (kartlegge > beskytte > detektere > respondere > gjenopprette)
- Abstrakte kategorier (organisatoriske, personell, fysiske, og teknologiske tiltak)
- Operasjonelle kategorier (f,eks. tiltak for tilgangskontroll, data/media-beskyttelse, IAM, nettverkssikkerhet, system/applikasjonssikkerhet, hendelsesrespons, opplæring, leverandørsikkerhet etc.)

For hver standard/veileder nedenfor, spesifiser hvilken kategorisering den benytter.

a. ISO/IEC 27002:2022 Information security controls
b. NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
c. NSMs Grunnprinsipper for IKT-sikkerhet
d. NIST Cyber Security Framework
e. CIS Critical Security Controls

Løsningsforslag

a. ISO/IEC 27002:2022 er strukturert med følgende **abstrakte tiltakskategorier:**
   1. Organisatoriske sikkerhetstiltak
   2. Tiltak for personellsikkerhet
   3. Fysiske sikkerhetstiltak
   4. Teknologiske sikkerhetstiltak

   Legg merke til at tidligere utgaver ISO/IEC 27002 var strukturert med spesifikke tiltakskategorier.

b. NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations er strukturert med følgende **operasjonelle tiltakskategorier:**
   1. ACCESS CONTROL
   2. AWARENESS AND TRAINING
   3. AUDIT AND ACCOUNTABILITY
   4. ASSESSMENT, AUTHORIZATION, AND MONITORING
   5. CONFIGURATION MANAGEMENT
   6. CONTINGENCY PLANNING
   7. IDENTIFICATION AND AUTHENTICATION
   8. INCIDENT RESPONSE
   9. MAINTENANCE
   10. MEDIA PROTECTION
   11. PHYSICAL AND ENVIRONMENTAL PROTECTION
   12. PLANNING
   13. PROGRAM MANAGEMENT
   14. PERSONNEL SECURITY
   15. PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY
   16. RISK ASSESSMENT
   17. SYSTEM AND SERVICES ACQUISITION
   18. SYSTEM AND COMMUNICATIONS PROTECTION
   19. SYSTEM AND INFORMATION INTEGRITY
   20. SUPPLY CHAIN RISK MANAGEMENT

c. NSMs Grunnprinsipper for IKT-sikkerhet er strukturert etter følgende **prosessorienterte kategorier:**
    1. Identifisere og kartlegge
    2. Beskytte og opprettholde
    3. Oppdage
    4. Håndtere og gjenopprette

d. NIST Cyber Security Framework er strukturert etter følgende **prosessorienterte kategorier** (som kalles «functions»):
    1. IDENTIFY
    2. PROTECT
    3. DETECT
    4. RESPOND
    5. RECOVER

e. CIS Critical Security Controls er strukturert etter følgende **operasjonelle tiltakskategorier:**
    1. Inventory and Control of Enterprise Assets
    2. Inventory and Control of Software Assets
    3. Data Protection
    4. Secure Configuration of Enterprise Assets and Software
    5. Account Management
    6. Access Control Management
    7. Continuous Vulnerability Management
    8. Audit Log Management
    9. Email and Web Browser Protections
    10. Malware Defenses
    11. Data Recovery
    12. Network Infrastructure Management
    13. Network Monitoring and Defense
    14. Security Awareness and Skills Training
    15. Service Provider Management
    16. Application Software Security
    17. Incident Response Management
    18. Penetration Testing